IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

ANGELA GROSS and MARK CHHABRIA, i*ndividually and on behalf of all others similarly situated*, Plaintiffs, v. ZEBRA STRATEGIES, INC., Defendant.	Case No._____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Angela Gross and Mark Chhabria ("Plaintiffs"), individually and on behalf of all others similarly situated (the "Class" or "Class Members"), bring this Class Action Complaint (the "Complaint") against Defendant Zebra Strategies, Inc. ("Zebra" or "Defendant"). The allegations set forth in this Complaint are based on the personal knowledge of the Plaintiffs and upon information and belief and further investigation of counsel.

I. NATURE OF THE ACTION

1. This is a data breach class action against Defendant for its failure to adequately secure and safeguard confidential and sensitive information held during the typical course of its business. Defendant's failure resulted in the theft and subsequent unauthorized sale of Plaintiffs' and Class Members sensitive information.

2. Zebra is a "qualitative and quantitative market research and strategy firm specializing in marginalized, vulnerable, and hard-to-reach populations."[1]

3. While much of the information regarding the incident remains in the exclusive control of Defendant, upon information and belief, an unauthorized employee or employees gained

[1] *Who We Are*, Zebra Strategies, https://zebrastrategies.com/about/ (last visited Aug. 26, 2024).

unauthorized access to Defendant's network and computer systems for an unknown period of time and obtained, exfiltrated, stole, and sold for profit Plaintiffs' and Class Members sensitive personal information (the "Data Breach").

4. Upon information and belief, the personal information of at least 20,000 individuals was affected by the Data Breach. The data accessed, exfiltrated, stolen, and sold by an unauthorized employee in the Data Breach consisted of Plaintiffs' and the Class Members' sensitive information—including names, contact information, and sensitive market survey responses—such as those related to medical conditions and status. Collectively, the information described in this paragraph shall be referred to as "Private Information" throughout this Complaint.

5. On June 18, 2024, Zebra announced the following Data Breach via email to its survey participants ("Notice of Incident"):

> **What Happened?**
>
> It was recently discovered that a former employee(s) accessed a database of research participants without authority and downloaded the data for an unauthorized use of that database. Your name was in that database, along with other personal information you shared with us. Your name and information may have been shared with a competitor(s) of Zebra Strategies to participate in paid research studies not conducted by ZEBRA.

6. Defendant had numerous statutory, contractual, and common law duties and obligations, including those based on its affirmative written representations and promises to Plaintiffs and the Class, to keep their Private Information confidential, safe, secure, and protected from unauthorized access, disclosure, exfiltration, or theft.

7. At all relevant times, Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality and security of their Private Information.

8. Further, Plaintiffs and Class Members reasonably expected Defendant to keep their Private Information confidential and secure, to use this information only for the business purposes they authorized, and to make only authorized disclosures of this information.

9. However, upon information and belief, Defendant acted negligently in its data security operations and breached numerous duties through one or more of the following acts or omissions: failing to implement and maintain reasonable safeguards—including a lack of encryption, poor access controls, lack of user verification or two factor authentication; failing to comply with industry-standard data security practices and federal and state laws and regulations governing data security; failing to properly train its employees on data security measures and protocols; failing to timely recognize and detect unauthorized parties accessing its system and that substantial amounts of data had been compromised; and failing to timely and adequately notify the impacted Class.

10. As a direct and proximate result of Defendant's breach, Defendant's employee was able to access areas of Defendant's network and remove files with the specific intent to sell and profit from Plaintiffs' and Class Members' sensitive information in illicit data markets.

11. Subsequently, two of Defendant's employees sold to, or otherwise illicitly transferred to, third parties including other research companies Sago, Inc and Accurate Market Research. This sale or transfer occurred without the consent of Plaintiffs or any Class Members and resulted in the dissemination of their Private Information to an unknown number of unauthorized parties.

12. In light of these events, Defendant has filed a lawsuit against its former employees who facilitated the illicit transfer. *See Zebra Strategies, Inc. v. Ada Gonzalez Nazario*, No. 1:24-cv-04146, ECF No. 53 (S.D.N.Y. July 16, 2024). In this action, Defendant seeks, *inter alia*, to

recover any proceeds its former employees obtained from the unauthorized sale of Plaintiffs and Class Members' Private Information. Additionally, Defendant seeks to recover the value of this Private Information, which it estimates at $2,100,000.

13. By implementing and maintaining reasonable safeguards and complying with standard data security practices, Defendant could have prevented the Data Breach and the unauthorized sale of the Plaintiffs and Class Members Private Information.

14. Plaintiffs bring this action on behalf of themselves and all persons whose Private Information was accessed, exfiltrated, and sold because of Defendant's failure to adequately protect the Private Information its customers entrusted to it; Defendant's failure to warn its current, former, and potential customers; and Defendant's failure to effectively monitor its network for security incidents.

15. As a result of the Data Breach, Plaintiffs and Class Members suffered harm and ascertainable losses, including but not limited to, a breach of contract, a loss of privacy, and the lost or diminished inherent value of their Private Information. Furthermore, Plaintiffs suffered emotional distress, fear, anxiety, nuisance and annoyance related to the theft and compromise of their Private Information. Also, Plaintiffs have incurred statutory and actual damages.

16. Plaintiffs seek to remedy these harms and prevent any future data compromise, individually and on behalf of all similarly situated persons whose Private Information was compromised and stolen as a result of the Data Breach and remains at risk due to inadequate data security practices employed by Defendant.

17. Accordingly, Plaintiffs, individually and on behalf of the Class, assert claims for Negligence, Breach of Express Contract, Breach of Implied Contract, Unjust Enrichment, violation

of the California Consumer Privacy Act ("CCPA"), Constructive Trust, and Declaratory and Injunctive relief.

II. PARTIES

18. Plaintiff Angela Gross is a natural person and citizen of California. She resides in San Francisco, California, where she intends to remain. According to an email she received from Zebra, Ms. Gross's Private Information was impacted in the Data Breach.

19. Plaintiff Mark Chhabria is a natural person and citizen of California. He resides in Marin County, California, where he intends to remain. According to an email he received from Zebra, Mr. Chhabria's Private Information was impacted in the Data Breach.

20. Defendant Zebra Strategies, Inc. is a for-profit market research and strategy company incorporated under the laws of the State of New York with its principal place of business located at 2090 Adam Clayton Powell Jr. Blvd., New York, NY 10027.

21. Defendant collected and continues to collect the Private Information of its customers and survey participants throughout its usual course of business operations.

22. By obtaining, collecting, using, and deriving benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties to those persons, and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

III. JURISDICTION AND VENUE

23. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d), *et seq*. The amount in controversy exceeds $5 million, exclusive of interest and costs. There are more than 100 members in the proposed Class, and at least one

member of the Class is a citizen of a state different from Defendant, including Plaintiffs. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

24. This Court has personal jurisdiction over Defendant because Defendant's principal places of business is located within this District and Defendant conducts substantial business in this district.

25. Venue is proper in this Court under 28 U.S.C. § 1391, because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District, and Defendant's principal place of business is within this judicial district.

IV. FACTUAL ALLEGATIONS

A. Background

26. In the ordinary course of its business practices, Defendant collects, stores, maintains, and uses individuals' Private Information, including that of Plaintiffs and Class Members. Such information includes, but is not limited to, names, addresses, and survey responses, which, in many cases, include health information and other sensitive personal information.

27. Plaintiffs and Class Members signed up with Defendant to respond to surveys and participate in market research for compensation and Defendant promised to maintain the confidentiality of Plaintiffs' and Class Members' information and to not share or sell the sensitive personal information.[2]

28. Defendant understands the importance of securely storing and maintaining Private Information.

29. Upon information and belief, Defendant became aware of the Data Breach in or around September 2023.

[2] https://money4talk.com/about/ (Aug. 26, 2024).

30. Defendant then took steps to retain independent cybersecurity experts to investigate the matter further but neglected to notify all affected individuals of the incident until on or about June 18, 2024. At that time, Defendant sent Plaintiffs and Class Members a brief email notice regarding the incident but largely omitted the types and extent of information involved in the Data Breach.

31. In its Notice of Incident, Defendant stated that it had "recently discovered that a former employee(s) accessed a database of research participants without authority and downloaded the data for an unauthorized use of that database."

32. The Notice disclosed that Plaintiffs' names and other personal information was included in the database but did not disclose the types and extent of information involved in the Data Breach.

33. Additionally, though Plaintiffs and the Class have an interest in ensuring that their information remains protected, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures taken by Defendant to ensure a data breach does not occur again, have not been shared with Plaintiffs or the Class.

34. In its Privacy Policy Defendant promised to "keep client information secure at all times, and prevent the misuse and unauthorized disclosure of it by [its] employees or any third parties."[3]

35. Defendant further promised that "[a]ll responses to [its] research are completely confidential. [Defendant] collects data in [its] studies for research purposes only, and [its] use of that information will be limited to that purpose."[4]

[3] *Privacy Policy*, Zebra Strategies, Inc., https://money4talk.com/privacy-policy/ (last visited Aug. 26, 2024).
[4] *Id.*

36. Defendant had and continues to have obligations created by implied and express contract, industry standards, common law, and representations made to Plaintiffs and the Class, to keep their Private Information private and confidential and to protect it from unauthorized access and potential disclosure.

37. Plaintiffs and the Class provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to employ reasonable care to keep such information confidential and secure from unauthorized access.

38. Defendant knew, or should have known, the importance of safeguarding the Private Information of Plaintiffs and Class Members, including their names, phone numbers, emails, and sensitive survey responses, and of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant harms that would be imposed on Plaintiffs and Class Members as a result of a breach.

39. The injuries to Plaintiffs and Class were directly and proximately caused by Defendant's own failure to install, implement or maintain adequate data security measures, software and other industry best practices for safeguarding the Private Information of Plaintiffs and Class Members.

B. Defendant Failed to Comply with FTC Guidelines

40. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable and adequate data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

41. In 2022, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines

note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; watch for data being transmitted from the system; and have a response plan ready in the event of a breach.[5]

42. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

43. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

44. Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer

[5] Ritchie, J. N. & A., & Jayanti, S.F.-T. and A. (2022, April 26). *Protecting personal information: A guide for business.* Federal Trade Commission. https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed October 27, 2023).

Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

45. At all relevant times, Defendant was fully aware of its obligation to protect the Private Information of consumer survey participants. Defendant was also aware of the significant repercussions that would result from its failure to do so.

46. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent or mitigate the Data Breach.

C. Plaintiffs' and Class Members' Damages

47. Defendant has failed to provide any compensation for the unauthorized release and disclosure of Plaintiffs' and the Class's Private Information.

48. Plaintiffs and the Class have been damaged by the disclosure and sale of their Private Information in the Data Breach.

49. Notably, Plaintiffs and Class Members suffered a loss of value of their Private Information when it was acquired, disclosed, and sold to a competitor. While the exact price for which Plaintiffs' and Class Members' information was sold remains unknown, the Defendant's own calculations value this Private Information at $2,100,000. *See Zebra Strategies Inc. v. Ada Gonzalez Nazario*, et al., ECF No. 53 (S.D.N.Y. July 16, 2024), ¶ 81.

50. Moreover, Plaintiffs and the Class have an ongoing interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further disclosures by the implementation of proper and adequate security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal information is password protected, or encrypted.

51. As a direct and proximate result of Defendant's actions and inaction, Plaintiffs and the Class have suffered anxiety, emotional distress, and loss of privacy because of the Data Breach.

D. Plaintiff Angela Gross's Experience

52. Plaintiff Gross regularly participates in market research for compensation.

53. Plaintiff Gross entered into a written contract with Defendant to participate in surveys and focus groups in exchange for monetary compensation.

54. As a specific term of the contract, Defendant represented, promised, and agreed to a limited scope of use of Plaintiff Gross' data. Specifically, Defendant promised in its Privacy Policy to keep all responses to research "completely confidential."[6] Further, Defendant represented that it collects "data in [its] studies for research purposes only, and [its] use of that information will be limited to that purpose."[7]

55. At all relevant times, Plaintiff Gross has been an active participant in commercial data markets. Prior to contracting with any business, she considers the scope of the transaction and use of her data and the data security representations of the firms to which she sells and provides her data. Prior to contracting with Defendant, she agreed to its Privacy Policy and considered the types of information she would provide Defendant in light thereof.

56. To maximize the value of her Private Information and preserve the scarcity of her data, Plaintiff Gross relied heavily on Defendant's promises to maintain the confidentiality of her data and to ensure her valuable sensitive Private Information is not freely shared on the data markets.

---

[6] *Privacy Policy*, Zebra Strategies, Inc., https://money4talk.com/privacy-policy/ (last visited Aug. 26, 2024).
[7] *Id.*

57. Relying on Defendant's numerous promises never to share or disclose her Private Information, Plaintiff contracted with Defendant and Defendant's market research affiliate Money4Talk.

58. Plaintiff relied on Defendant's promise to maintain her Private Information in a "completely confidential" manner and to use her data "for research purposes only" when she signed up to participate in Defendant's market research campaigns. Plaintiff entrusted her Private Information and other confidential information to Defendant with the reasonable expectation and understanding that Defendant, or its agents, would take at least industry-standard precautions to protect, maintain, and safeguard that information from unauthorized use or disclosure, and would timely notify her of any data security incidents related to her Private Information. Plaintiff Gross would not have agreed to participate in Defendant's market research had she known that Defendant would not take reasonable steps to safeguard her Private Information.

59. Plaintiff Gross provided Defendant with her name, address, email, phone number, and demographic information. Further, she responded to surveys and provided information regarding her medical history, and consumer and political preferences.

60. On or around June 18, 2024, Plaintiff Gross received an email titled "Important Information from Zebra Strategies" with the following message:

> It was recently discovered that a former employee(s) accessed a database of research participants without authority and downloaded the data for an unauthorized use of that database. Your name was in that database, along with other personal information you shared with us. Your name and information may have been shared with a competitor(s) of Zebra Strategies to participate in paid research studies not conducted by ZEBRA.

61. As a result of the Data Breach, Plaintiff Gross was forced to spend time dealing with and responding to the direct consequences of the Data Breach. These remedial measures included spending time on telephone calls, researching the Data Breach, and contacting Defendant

to determine exactly what information was accessed and exfiltrated from Defendant's network. This is uncompensated time that has been lost forever and cannot be recaptured.

62. Moreover, Plaintiff Gross has suffered actual injury in the form of damages to, and diminution in, the value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant and that she takes very seriously. Through the subsequent sale of her Private Information into the data markets without her consent, her Private Information lost its scarcity, and its value has been destroyed or diminished, as a result of the Data Breach.

63. Plaintiff Gross has a continuing interest in ensuring that her Private Information which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches.

64. Plaintiff Gross also has a continuing interest in ensuring that the monetary value of her Private Information that was realized through the sale of her data is rightfully protected and returned to her and the Class Members.

E. Plaintiff Mark Chhabria's Experience

65. Plaintiff Chhabria regularly participates in market research for compensation.

66. Plaintiff Chhabria signed up with Defendant to participate in surveys and focus groups in exchange for monetary compensation.

67. Plaintiff Chhabria is very careful about which marketing firms he provides his data to and he researches and considers company reviews and the experiences of other users prior to signing up.

68. To maximize the value of his Private Information, Plaintiff Chhabria relies heavily on the research companies' promises to maintain the confidentiality of his data and responses to ensure his valuable Private Information is not freely shared on data markets.

69. Relying on Defendant's numerous promises never to share or disclose his Private Information, Plaintiff Chhabria signed up with Defendant's market research affiliate Money4Talk.

70. Plaintiff Chhabria relied on Defendant's promise to maintain his Private Information in a "completely confidential" manner and to use his data "for research purposes only" when he signed up to participate in Defendant's market research campaigns.

71. Plaintiff Chhabria recalls providing Defendant with his name, address, email, phone number, and demographic information. Additionally, he responded to surveys and provided information regarding his medical history, and consumer and political preferences.

72. On or around June 18, 2024, Plaintiff Chhabria received an email titled "Important Information from Zebra Strategies" with the following message:

> It was recently discovered that a former employee(s) accessed a database of research participants without authority and downloaded the data for an unauthorized use of that database. Your name was in that database, along with other personal information you shared with us. Your name and information may have been shared with a competitor(s) of Zebra Strategies to participate in paid research studies not conducted by ZEBRA.

73. Plaintiff Chhabria entrusted his Private Information and other confidential information to Defendant with the reasonable expectation and understanding that Defendant, or its agents, would take at least industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to his Private Information. Plaintiff Chhabria would not have agreed to participate in Defendant's market research had he known that Defendant would not take reasonable steps to safeguard his Private Information.

74. Plaintiff Chhabria has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which includes spending time on telephone calls and researching the Data Breach.

75. Plaintiff Chhabria has suffered actual injury in the form of damages to, and diminution in, the value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant and that he takes very seriously. Through the subsequent sale of his Private Information into the data markets without his consent, his Private Information lost its scarcity, and its value has been destroyed or diminished as a result of the Data Breach.

76. Plaintiff Chhabria has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of his privacy.

77. Additionally, Plaintiff Chhabria does not recall having been involved in any other data breaches in which his sensitive and confidential Private Information was compromised.

78. Plaintiff Chhabria has a continuing interest in ensuring that his Private Information which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches.

V. CLASS ACTION ALLEGATIONS

79. Plaintiffs bring this nationwide class action according to Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4).

80. The nationwide Class that Plaintiffs seek to represent is defined as follows:

> All persons residing in the United States whose Private Information was accessed and exfiltrated in the Data Breach that Defendant sent Notice of on or about June 18, 2024 (the "Class").

81. Plaintiff Angela Gross also seeks to represent a California Subclass defined as follows:

> All persons residing in the State of California whose Private Information was accessed and exfiltrated in the Data Breach that Defendant sent Notice of on or about June 18, 2024 (the "California Subclass").

82. Excluded from the Classes are: (i) Defendant and its employees, officers, directors, affiliates, parents, subsidiaries, and any entity in which Defendant have a whole or partial ownership of financial interest; (ii) all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; (iii) any counsel and their respective staff appearing in this matter; and (iv) all judges assigned to hear any aspect of this litigation, their immediate family members, and their respective court staff.

83. Plaintiffs reserve the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

84. **Numerosity**. The Class is so numerous that joinder of all members is impracticable. The Class includes thousands of individuals whose personal data was compromised by the Data Breach. The exact number of Class members is in the possession and control of Defendant and will be ascertainable through discovery, but Zebra has disclosed that approximately 20,000 individuals' Private Information was involved in the Data Breach.

85. **Commonality.** There are numerous questions of law and fact common to Plaintiffs and the Class that predominate over any questions that may affect only individual Class members, including, without limitation:

- Whether Defendant unlawfully maintained, lost or disclosed Plaintiffs' and the Class's Private Information;
- Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

- Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- Whether Defendant owed a duty to Class to safeguard their Private Information;
- Whether Defendant breached duties to Class to safeguard their Private Information;
- Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- Whether Defendant owed a duty to provide Plaintiffs and Class timely notice of this Data Breach, and whether Defendant breached that duty;
- Whether Plaintiffs and Class suffered legally cognizable damages as a result of Defendant's misconduct;
- Whether Defendant's conduct was negligent;
- Whether Defendant's conduct violated federal law;
- Whether Defendant's conduct violated state law; and
- Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

86. **Typicality**. Plaintiffs' claims are typical of the claims of the Class in that Plaintiffs, like all proposed Class members, had their Private Information compromised, breached, or otherwise stolen in the Data Breach. Plaintiffs and the Class were injured through the uniform misconduct of Defendant, described throughout this Complaint, and assert the same claims for relief.

87. **Adequacy**. Plaintiffs and counsel will fairly and adequately protect the interests of Plaintiffs and the proposed Class. Plaintiffs retained counsel who are experienced in class action and complex litigation, particularly those involving data breaches like the one at issue in this class

action complaint. Plaintiffs have no interests that are antagonistic to, or in conflict with, the interests of other Class members.

88. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class Members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy such that, in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied. Plaintiffs and the Class have been harmed by Defendant's wrongful conduct and/or inaction. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Defendant's conduct and/or inaction. Plaintiffs know of no difficulties implicated in this litigation that would preclude its maintenance as a class action.

89. Class certification is appropriate under Fed. R. Civ. P. 23(b)(1)(A) because the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual members of the Class, which would establish incompatible standards of conduct for Defendant. In contrast, the treatment of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each Class Member. Specifically, in the absence of class treatment, injunctive relief could be entered in multiple cases, but the ordered relief may vary, forcing Defendant to choose between differing means of upgrading its data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by Class members would create the risk of adjudications with respect to individual Class Members that, as

a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

90. Class certification, therefore, is appropriate under Rule 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

91. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed its legal duty or obligation to Plaintiffs and the Class to exercise due care in collecting, storing, using, safeguarding, or otherwise maintaining their Private Information;

b. Whether Defendant breached its legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, using, safeguarding, or otherwise maintaining their Private Information;

c. Whether Defendant failed to comply with its own policies or procedures and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether Plaintiffs and the Class are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

VI. CAUSES OF ACTION

COUNT I
Negligence
(On behalf of Plaintiffs and the Class)

92. Plaintiffs and the Class re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

93. Plaintiffs and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their Private Information for business purposes only, and not disclose their Private Information to unauthorized third parties.

94. Defendant owed a duty to Plaintiffs and the Class to exercise reasonable care in obtaining, using, maintaining, and protecting their Private Information from unauthorized third parties.

95. The legal duties owed by Defendant to Plaintiffs and the Class include, but are not limited to, the following:

a. To exercise reasonable care in procuring, retaining, securing, safeguarding, deleting, and protecting the Private Information of Plaintiffs and the Class in Defendant's possession;

b. To protect the Private Information of Plaintiffs and the Class in Defendant's possession through the use of reasonable and adequate security procedures that comply with industry-standard practices; and

c. To implement processes and software to quickly detect a data breach and to act timely on warnings about data breaches, including the prompt notification of Plaintiffs and Class Members of such data breach.

96. Defendant breached its duties to Plaintiffs and the Class. Defendant knew or should have known the risks of collecting and storing Private Information and the importance of maintaining secure systems, especially considering the recent prevalence of data breaches and cyber-attacks.

97. Defendant knew or should have known that its security practices did not adequately safeguard the Private Information of Plaintiffs and the Class.

98. Through Defendant's acts and omissions described in this Complaint—including Defendant's failure to provide adequate security measures and its failure to protect the Private Information of Plaintiffs and the Class from foreseeable capture, access, exfiltration, theft, disclosure, and misuse—Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiffs and the Class.

99. Defendant was subject to an independent duty, untethered to any contract between Defendant and Plaintiffs and the Class.

100. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose when Plaintiffs and the Class entrusted Defendant with their confidential Private Information.

101. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the Class. Upon information and belief, Defendant's misconduct included, but was not limited to, its

failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for safekeeping of the Private Information of Plaintiffs and the Class.

102. Defendant was in the best position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

103. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the Private Information of Plaintiffs and the Class.

104. Defendant breached its duties to Plaintiffs and Class Members in several ways, including:

- Failing to implement adequate security systems, protocols, and practices sufficient to protect customers' Private Information and thereby creating a foreseeable risk of harm;
- Failing to comply with the minimum industry data security standards during the period of the Data Breach;
- Failing to act despite knowing or having reason to know that its systems were vulnerable to attack; and
- Failing to timely and accurately disclose to customers that their Private Information had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

105. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and Class Members and the harm and substantial risk of imminent harm suffered by Plaintiffs and the Class. The Private Information of Plaintiffs and the Class was stolen and accessed as a proximate result of Defendant's failure to

exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

106. Due to Defendant's negligence, Plaintiffs and the Class suffered injuries including the lost or diminished value of their Private Information.

107. These injuries were reasonably foreseeable given the nature of the Private Information and the manner in which Defendant handled it. The injury and harm that Plaintiffs and the Class suffered was the direct and proximate result of Defendant's negligent conduct.

108. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class are entitled to recover actual, consequential, and/or nominal damages.

COUNT II
Breach of Express Contract
(On Behalf of Plaintiffs and the Class)

109. Plaintiffs and the Class re-allege and incorporate by reference the paragraphs above as if fully re-written herein.

110. Defendant's Privacy Policy constitutes an agreement between Defendant and individuals who provided Private Information to Defendant, whether directly or indirectly, including Plaintiffs and Class Members.

111. Defendant's Privacy Policy prominently declares Defendant's commitment to "protecting the privacy of [its] clients and research participants," including Plaintiffs and Class Members. Defendant asserts that its Privacy Policy applies to all "personal information [it] collect[s] or use[s] in the course of conducting [its] business" as well as all "research participant data housed in a Zebra Strategies facility or stored on the Zebra Strategies network."

112. Defendant's Privacy Policy promises, *inter alia*, that "[a]ll responses to [its] research are completely confidential" and that Defendant "collect[s] data in [its] studies for research purposes only, and [Defendant's] use of that information will be limited" to that purpose.

113. Defendant's Privacy Policy also states that "[a]nyone who has access to [Private Information], or data must follow this privacy policy."

114. Plaintiffs and Class Members formed a contract with Defendant when they provided Private Information to Defendant subject to the Privacy Policy in exchange for monetary compensation.

115. Defendant breached its agreement with Plaintiffs and Class Members by failing to maintain the confidentiality of the Private Information under the terms of the Privacy Policy.

116. As a direct and proximate result of Defendant's breach of express contract, Plaintiffs and the Class have suffered, and will continue to suffer, from the diminution or wholesale destruction of the value of their Private Information.

117. As a direct and proximate result of Defendant's breach of express contract, Plaintiffs and the Class are entitled to recover actual, consequential, and/or nominal damages.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

118. Plaintiffs and the Class re-allege and incorporate by reference the paragraphs above as if fully re-written herein.

119. Plaintiffs and the Class entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect Plaintiffs' and Class Members' Private Information and to timely notify Plaintiffs and Class Members if their Private Information was compromised.

120. Defendant solicited, offered, and invited Plaintiffs and Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers when they provided their Private Information in exchange for valuable consideration.

121. Defendant accepted possession of Plaintiffs' and Class Members' Private Information for Defendant's own business benefit.

122. When Plaintiffs and Class Members provided their Private Information to Defendant in exchange for monetary compensation, they entered into implied contracts with Defendant.

123. Plaintiffs and Class Members entered into these implied contracts with the reasonable expectation that Defendant's data security practices and policies complied with industry standards and provided a reasonable bulwark against unauthorized access of their Private Information.

124. Defendant's implied promises included, but were not limited to:

- Taking steps to ensure that any agents or employees who were granted access to the Private Information also protect the confidentiality of that data;
- Taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve a legitimate purpose;
- Applying proper encryption;
- Designing and implementing appropriate collection and retention policies to protect information against unauthorized access; and
- Other steps to protect against foreseeable data breaches.

125. Defendant's implied promises to safeguard Plaintiffs' and Class Members' Private Information are evidenced by, *e.g.*, representations in Defendant's Privacy Policy described above.

126. Plaintiffs and the Class fully performed their obligations under their implied contracts with Defendant.

127. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of an implicit contract whereby Defendant agreed to safeguard the confidentiality of Plaintiffs' and Class Members' Private Information.

128. Had Defendant disclosed to Plaintiffs and the Class that it did not have adequate security practices to protect the confidentiality of sensitive data, Plaintiffs and the other Class Members would not have provided their Private Information to Defendant.

129. Defendant breached the implied contract with Plaintiffs and the Class by failing to safeguard and protect their Private Information and by failing to provide timely and accurate notice to them that their Private Information was compromised as a result of the Data Breach.

130. As a direct and proximate result of Defendant's breach of implied contract, Plaintiffs and the Class have suffered, and will continue to suffer, from the diminution or wholesale destruction of the value of their Private Information.

131. As a direct and proximate result of Defendant's breach of implied contract, Plaintiffs and the Class are entitled to recover actual, consequential, and/or nominal damages.

COUNT IV
Unjust Enrichment
(On behalf of Plaintiffs and the Class)

132. Plaintiffs and the Class re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

133. Plaintiffs bring this claim in the alternative to the breach of express contract and breach of implied contract claims above.

134. Plaintiffs and the Class conferred a monetary benefit on Defendant by providing Defendant with their valuable Private Information, which Defendant knowingly used or retained in the course of its business.

135. Defendant benefited from and was enriched by receiving Plaintiffs' and the Class Members' Private Information and through its use of that information for its own financial and business benefit and profit. Defendant understood this benefit and accepted the benefit knowingly.

136. Defendant also understood and appreciated that the Private Information of Plaintiffs and the Class was private and confidential and that its value depended upon Defendant maintaining the privacy and confidentiality of that Private Information.

137. Defendant's express and implicit representations to Plaintiffs and Class Members created the reasonable expectation that it had adequate data security procedures to protect the confidentiality of sensitive Private Information.

138. Indeed, in its Privacy Policy—on which Plaintiffs and Class Members relied in disclosing their Private Information—Defendant promised that it would maintain the confidentiality of Plaintiffs and Class Members' Private Information. Further, Defendant represented that its "use of [Plaintiffs and Class Members' Private Information] will be limited to [research purposes]."

139. However, rather than provide a reasonable level of security that would have prevented the Data Breach, Defendant sought to avoid its data security obligations by utilizing cheaper, ineffective security measures.

140. Defendant's decision to shirk its data security obligations came directly at the expense of Plaintiffs and Class Members. Plaintiffs and the Class suffered injuries as a direct and proximate result of Defendant's failure to provide the requisite data security.

141. But for Defendant's willingness and commitment to maintain its privacy and confidentiality, the Private Information would not have been transferred to and entrusted to Defendant. Indeed, if Defendant had disclosed the inadequacy of its data and cyber security measures, it would not have been permitted to continue in operation by regulators, its clients, and its consumers.

142. As a result of Defendant's failure to disclose the truth regarding its data security practices, Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and the Class. Defendant profited and continues to profit from its retention and use of their Private Information while its value to Plaintiffs and the Class has been diminished or wholly destroyed.

143. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged in this complaint, including the compilation, use, and retention of Plaintiffs' and the Class Members' Private Information, while at the same time failing to maintain said information securely from intrusion and theft by cyber criminals, hackers and identity thieves—all despite its express and implied representations to the contrary.

144. Plaintiffs and the Class have no adequate remedy at law.

145. Under traditional principles of equity and good conscience, Defendant should not be permitted to retain the benefits and profits it received and continues to receive from its use of Plaintiffs' and Class Members' Private Information in this unjust manner. Defendant acquired Plaintiffs' and Class Members' Private Information, as well as its concomitant monetary value,

through inequitable means by failing to disclose the inadequate security practices previously alleged.

146. Despite obtaining Plaintiffs' and Class Members' Private Information pursuant to misrepresentations about the state of its data security practices, Defendant used Plaintiffs' and Class Members' Private Information to generate revenue and reap profits in the course of its business. Indeed, Defendant has stated that it values Plaintiffs' and Class Members' Private Information at $2,100,000. *See Zebra v. Gonzalez Nazario*, No. 1:24-cv-04146, ECF No. 53, (S.D.N.Y. July 16, 2024) ¶ 84.

147. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and the Class, any and all proceeds and profits that it unjustly received from the use of Plaintiffs' and Class Members' Private Information.

COUNT V
California Consumer Privacy Act
Cal. Civ. Code § 1798.100, *et seq.*
(On Behalf of Plaintiff Angela Gross and the California Subclass)

148. Plaintiff Gross and the California Subclass re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

149. Plaintiff Gross brings this claim individually and on behalf of the California Subclass for violation of the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100, *et seq.* ("CCPA").

150. Plaintiff Gross and the California Subclass Members are consumers and California residents as defined by Cal. Civ. Code § 1798.140(i).

151. Defendant is a "business" as defined by Civ. Code § 1798.140(d) because it is a corporation that collects consumers' personal information, determines the purposes and means of processing said consumers' information, does business in the state of California, and "[d]erives 50 percent or more of its annual revenues from selling or sharing consumers' personal information." Cal. Civ. Code § 1798.140(d)(1)(C).

152. Specifically, Defendant obtains and collects consumers' Personal Information when research participants engage with its research projects.

153. Defendant and its customers determine the purposes and means of processing consumers' Personal Information. Defendant uses consumers' personal data to provide services at its customers' request, as well as in the development, improvement, and evaluation of Defendant's own services.

154. The CCPA states that "Personal Information" includes "[a]n individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted . . . (iv) Medical information." Cal. Civ. Code §§ 1798.150(a)(1) and 1798.81.5(d)(1)(A).

155. "Medical Information" encompasses any individually identifiable information "regarding the individual's medical history or medical treatment or diagnosis by a healthcare professional." Cal. Civ. Code § 1798.81.5(d)(1)(A)(iv).

156. Plaintiff Gross and California Subclass Members' names, in combination with Medical Information and other sensitive Private Information compromised in the Data Breach, constitutes "Personal Information" within the meaning of the CCPA.

157. Because of the Data Breach, Plaintiff's and California Subclass Members' Personal Information was accessed without authorization, exfiltrated, and stolen in a nonencrypted and/or nonredacted format.

158. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

159. Defendant violated § 1798.150 of the CCPA by failing to protect Plaintiff's and California Subclass Members' nonencrypted Personal Information from unauthorized access and exfiltration, theft, or disclosure in violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

160. Defendant had a duty to implement and maintain reasonable security practices to protect Plaintiff and California Subclass Members' Personal Information. As detailed herein, Defendant failed to do so.

161. Defendant stored and maintained Plaintiff and the California Subclass' Personal Information in a form that allowed unauthorized parties to access it.

162. During the Data Breach, unauthorized parties accessed "nonencrypted and unredacted Personal Information" as defined in Cal. Civ. Code § 1798.81.5(A)(1)(d).

163. Defendant violated the CCPA by failing to protect Plaintiff and the California Subclass Members' Personal Information from unauthorized access and exfiltration, theft, or disclosure.

164. Plaintiff Gross and the California Subclass seek injunctive or other equitable relief to ensure that Defendant hereinafter adequately safeguards Personal Information in its possession by implementing reasonable security procedures and practices. This relief is important because Defendant still holds Personal Information related to Plaintiff and the California Subclass. Plaintiff

and the California Subclass have an ongoing interest in ensuring that their Private Information is reasonably protected.

165. Plaintiff Gross and the California Subclass Members seek statutory damages or actual damages, whichever is greater, pursuant to Cal. Civ. Code § 1798.150.

166. As a direct and proximate result of Defendant's violations of the CCPA, Plaintiff and the California Subclass Members suffered damages, as described above.

167. On August 26, 2024, Plaintiff's counsel sent Defendant a written notice of its violations of the CCPA along with a demand that such violations be cured. Defendant received this notice on August 29, 2024.

168. Over the 30 days following its receipt of the CCPA notice letter, Defendant failed to cure the effects of the Data Breach—which would have required retrieving the Personal Information or securing said information from continuing and future use. Accordingly, Plaintiff and the California Subclass seek all actual or compensatory damages according to proof or statutory damages allowable under the CCPA, whichever is higher. Plaintiff Gross and the California Subclass also seek such further relief as this Court may deem just and proper, including injunctive or declaratory relief.

COUNT VI
Constructive Trust
(On Behalf of Plaintiffs and the Class)

169. Plaintiffs and the Class re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

170. When Plaintiffs and the Class entrusted Defendant with their sensitive information, Defendant agreed—both implicitly and expressly in its Privacy Policy—to safeguard this information and prevent its unauthorized dissemination and disclosure.

171. Plaintiffs and the Class trusted that Defendant would comply with its own representations and promises concerning the confidentiality of their Private Information.

172. This entrustment created a confidential or fiduciary relationship between Plaintiffs and the Class on one side and the Defendant on the other.

173. In its Privacy Policy, Defendant stated that it was "committed to protecting the privacy" of Plaintiffs and the Class. Accordingly, Defendant promised to keep Plaintiffs and the Class's Private Information "completely confidential" and to use such information "for research purposes only." Plaintiffs and the Class relied on this express promise when they provided Defendant with their Private Information.

174. Further, in accepting Plaintiffs' and Class Members' Private Information, Defendant implicitly promised not to allow its employees to sell the information and allow for its widespread dissemination. Such unauthorized dissemination severely diminished or totally destroyed the monetary value of Plaintiffs' and the Class's Private Information.

175. Plaintiffs and the Class relied on Defendant's express and implied promises when they entrusted Defendant with their Private Information.

176. Had Plaintiffs and the Class known that Defendant did not intend to keep its promises but, rather, to store their Private Information in a woefully inadequate manner, Plaintiffs and the Class would not have agreed to give Defendant their Private Information.

177. Defendant is currently engaged in a lawsuit to recover the proceeds of the illicit sale of Plaintiffs' and the Class's Private Information. *See Zebra v. Gonzalez Nazario*, No. 1:24-cv-04146, ECF No. 53, (S.D.N.Y. July 16, 2024) ¶¶ 84, 90.

178. Defendant will retain a benefit if it recovers the proceeds of the unauthorized sale or transfer of Plaintiffs' and the Class Members' Private Information in the action mentioned above.

179. This benefit will come directly at the expense of Plaintiffs and the Class, who saw the value of their Private Information severely diminished or wholly destroyed as a result of the sale.

180. Finally, it would violate traditional notions of equity and good conscience to allow Defendant to keep the proceeds of this sale despite Defendant's failure to abide by either its own express and implied promises or the duties imposed upon it by statute or law. Defendant should not be allowed to retain such a benefit.

181. Consequently, Plaintiffs and the Class request that any award Defendant receives in *Zebra v. Gonzalez Nazario*, No. 1:24-cv-04146, ECF No. 53, (S.D.N.Y. July 16, 2024) be placed in constructive trust for the benefit of Plaintiffs and the Class.

COUNT VII
Declaratory Judgment and Injunctive Relief
(On Behalf of Plaintiffs and the Class)

182. Plaintiffs and the Class re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

183. Plaintiffs pursue this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

184. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further relief as necessary. Additionally, this Court has broad authority to restrain acts, such as those involved here, that are tortious and violate the terms of the federal statutes described in this Complaint.

185. An actual controversy exists regarding Defendant's present and prospective duties to reasonably safeguard Plaintiffs' and Class Members' Private Information, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from future data breaches that compromise their Private Information. Plaintiffs and the Class remain at imminent risk of additional unauthorized access of their Private Information.

186. In addition to a declaration of the parties' relative rights and legal relationship, this Court should issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect Private Information.

187. Further, this Court should issue injunctive relief requiring Defendant to delete, destroy, and purge the Private Information of Plaintiffs and Class Members unless Defendant can provide reasonable justification for the retention and continued use of such information that outweighs the privacy interests of Plaintiffs and Class Members.

188. Defendant still possesses the Private Information of Plaintiffs and Class Members.

189. As far as Plaintiffs are aware, Defendant has made no announcement that it has changed its data retention policies or practices relating to the Private Information.

190. There is no reason to believe that Defendant's employee training and data security measures are any more adequate now than prior to the breach. Nothing indicates that Defendant's current practices comply with its legal duties and obligations.

191. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of a subsequent data breach at Zebra. The risk of such a breach is real, immediate, and substantial.

192. As described above, Plaintiffs and Class Members have suffered actual harm in the wake of the Data Breach. Plaintiffs and Class Members face a risk of additional harm due to the

exposure of their Private Information and Defendant's failure to address the security failings that led to such exposure.

193. If an injunction is not issued, Plaintiffs and Class Members will suffer hardship that exceeds any harm to Defendant that will result from the issuance of an injunction. If another data breach occurs at Zebra, Plaintiffs and Class Members will likely suffer further diminution of the value of their Private Information and may be subjected to fraud, identity theft, and other harms. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable data security measures is relatively minimal. Further, Defendant has a pre-existing legal obligation to employ such measures.

194. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Zebra, thereby eliminating the additional injuries that would result to Plaintiffs and Class Members.

195. Plaintiffs, therefore, seek a declaration that (1) Defendant's existing data security measures do not comply with their explicit or implicit contractual obligations and duties of care to provide adequate data security, and (2) that to comply with their explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Conducting regular database scanning and security checks; and

e. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Angela Gross and Mark Chhabria, individually and on behalf of all others similarly situated, request judgment against Defendant and that the Court grant the following:

1. An order certifying the Class and appointing Plaintiffs and their counsel to represent the Class;

2. An order enjoining Defendant from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of the Private Information belonging to Plaintiffs and the Class;

3. Injunctive relief requiring Defendant to:

   a. Engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a

periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Engage third-party security auditors and internal personnel to run automated security monitoring;

c. Audit, test, and train its security personnel regarding any new or modified procedures;

d. Conduct regular database scanning and security checks;

e. Routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

4. An order instructing Defendant to purchase or provide funds for credit monitoring services for Plaintiffs and all Class Members;

5. An order instructing Defendant to purge or otherwise delete Plaintiffs' and Class Members' Private Information;

6. An award of compensatory, statutory, nominal, and punitive damages, in an amount to be determined at trial;

7. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

8. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

9. Any and all such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs hereby demand this matter be tried before a jury.

Respectfully submitted,

Dated: November 7, 2024

/s/ *Vicki J. Maniatis*

Vicki J. Maniatis, Esq.
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
405 East 50th Street
New York, New York 10022
Phone: (212) 594-5300
vmaniatis@milberg.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

Joseph M. Lyon*
Kevin M. Cox*
THE LYON FIRM
2754 Erie Ave.
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com
kcox@thelyonfirm.com

Attorneys for Plaintiffs and Putative Class

**Pro Hac Vice forthcoming*